WE CLAIM AS OUR INVENTION:

1. A method for protecting a security module, in which security-relevant data are stored, inserted on a device motherboard, comprising the steps of:

monitoring proper insertion of said security module on said device motherboard with a first function unit and a second function unit in said security module;

signaling at least one status of said security module with said first function unit; and

detecting at least one of improper use and improper replacement of said security module with said second function unit and, upon a detection of at least one of said improper use and said improper replacement, said second function unit causing said security-relevant data to be erased.

2. A method as claimed in claim 1 comprising the additional steps of:

following at least one of proper use and proper replacement of said security module, re-initializing, with said first function unit, any erased, security-relevant data; and

after said re-initializing, enabling each of said first function unit and said second function unit to re-commission said security module.

~~A method as claimed in claim 1 comprising the additional steps of:~~

normally operating said security module with system voltage from a device containing said device motherboard and, in an absence of said system voltage, operating said security module with a battery; and

monitoring a status of said battery with said second function unit as a basis for detecting at least one of said improper use and said improper replacement.

4. A method as claimed in claim 1 comprising providing a third function unit and inhibiting said security module with said third function unit during at least one of replacement of said security module on said device motherboard and damage to said security module.

5. A method as claimed in claim 4 comprising detecting said damage to said security module with said third function unit.

6. A method as claimed in claim 1 comprising evaluating a running time credit with said first function unit and, upon expiration of said time credit, signaling a suspicious status of said security module with said first function unit.

7. A method as claimed in claim 6 comprising the additional steps of:

after expiration of said time credit, said first function unit establishing a communication with a remote data source; and

restoring normal operation to said security module via said communication.

8. A method as claimed in claim 6 comprising selecting a duration of said time credit to obtain a time credit of selected duration, and loading said time credit of selected duration into a memory in said security module, said memory being accessible by said first function unit.

9. A method as claimed in claim 6 wherein said time credit is a first time credit, and comprising the additional steps of monitoring a second time credit with said first function unit, which is longer than said first time credit, and signaling a status designating a device containing said device motherboard as being inoperable when said second time credit expires.

10. A security module for insertion on a device motherboard, comprising:

a memory in which security-relevant data are stored;

a battery;

a connection to a system voltage of a device containing said device motherboard;

a first function unit and a second function unit;

a logic arrangement for supplying said first function unit and said second function unit with one of voltage from said battery and said system voltage;

said first function unit having a loadable memory in which a time credit is loaded, and said first function unit monitoring said time credit and having a signal element which signals expiration of said time credit; and

said second function unit detecting at least one of improper use and improper replacement of said security module and, upon detection of at least one of said improper use and said improper replacement, erasing said security-relevant data in said memory.

11. A security module as claimed in claim 10 wherein said second function unit comprises a voltage monitoring unit connected to said connection for system voltage and to said battery, said second function unit also being connected to said memory and supplying an operating voltage to said memory to maintain said security-relevant contents stored in said memory, and which erases said security-relevant contents by ceasing supply of said operating voltage to said memory.

12. A security module as claimed in claim 10 further comprising a third function unit having a test voltage line at which a voltage level is present, said third function unit inhibiting operation of said security module if said voltage level on said test voltage line deviates from a predetermined value, and said third function unit having self-holding capability for maintaining said inhibit status, and wherein said first function unit comprises a processor connected to said second function unit and said third function unit for signaling respective statuses of said security module dependent on signals from said second function unit and said third function unit.

13. A security module as claimed in claim 12 wherein said processor contains said memory and is supplied with said operating voltage from said second function unit

and which is connected to said system voltage, and which is connected to said third function unit to reset said third function unit via a first line and which is connected to said third function unit to interrogate a status of said third function unit via a second line.

14. A security module as claimed in claim 10 further comprising:

a printed circuit board on which said first function unit and said second function unit are mounted, said printed circuit board having terminals for said battery;

a security module housing formed by a hard casting compound surrounding said printed circuit board and said first function unit and said second function unit, with said contact terminals being exposed to an exterior of said housing;

said battery being replaceably connected to said contact terminals outside of said housing; and

said printed circuit board having a first contact group, accessible from outside of said housing, for communicating with a system bus of a device containing said device motherboard, and a second contact group accessible from an exterior of said housing for receiving said system voltage, and at least one of said first contact group and said second contact group being connected to said first function unit and said second function unit to monitor a plugged status of said security module and whether said security module is damaged.

15. A security module as claimed in claim 10 wherein said first function unit comprises a processor having output terminals connected to said signal element.

16. A security module as claimed in claim 15 wherein said signal element comprises an internal element in said security module connected to said processor.